Assignment IV: Cyber Attacks: Reconnaissance & Exploitation
VAPT using NMap, Nessus, Metasploit

Computer Security Lab

By Hiran V Nath, CSED NIT Calicut

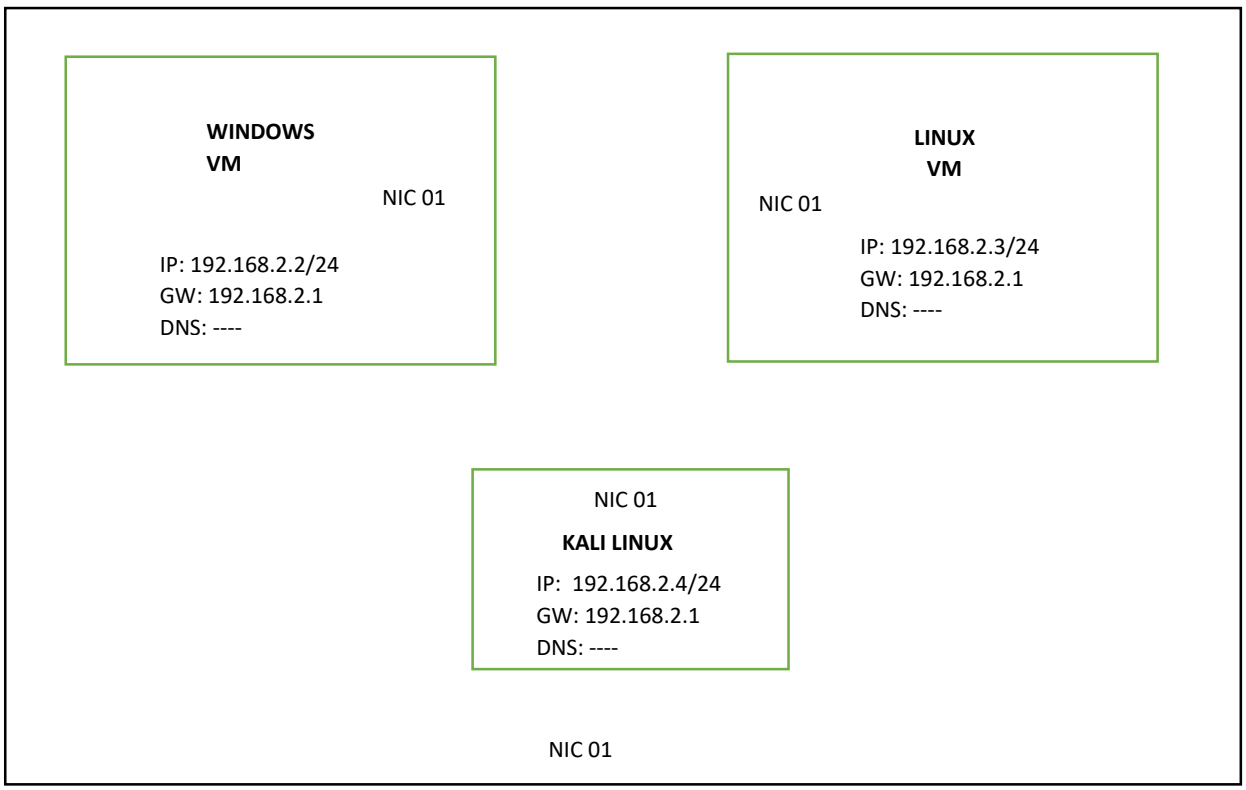
Submission: Nothing to be submitted

This assignment must be done individually. The assessment evaluation would be done based on an online quiz (followed by a viva based on the scenario).

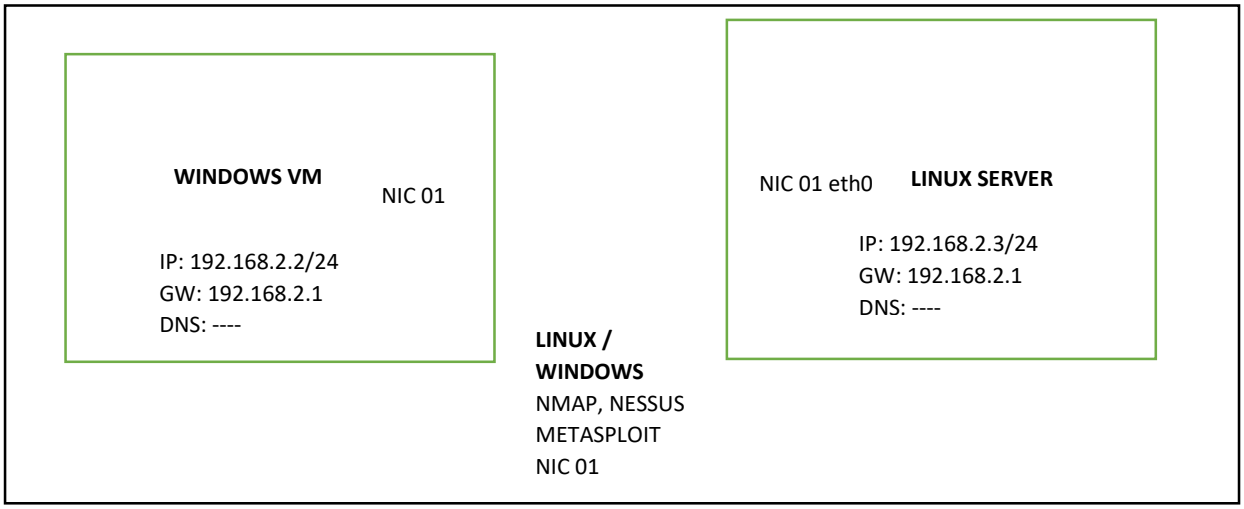
After completing this assignment, you will get a feeling of the methods taken by a hacker. This also gives some steps taken by a VAPT engineer/ CERT-In empanelled ethical hacker, but not all. In details, this assignment won't take care of all the steps taken by a skilled ethical hacker / VAPT engineer. The state sponsored hackers are employed by various organisations and have different aim. Their aim is for cyber espionage and the cyber-attacks happens between countries.

Now you could either use Kali Linux for doing this assignment as shown in first network diagram, or else you have to install Nmap / Zenmap, Nessus and Metasploit in your host system. These software are preloaded in Kali Linux. Your first activity is to understand how to carryout Reconnaissance of the network. For which you could use NMAP and Nessus, using various scanning options. You are allowed to use Zenmap, the GUI version of NMAP for Reconnaissance phase, but you should be knowing the options for doing the same with nmap command line also.

Network Diagram – with Static IP addressing - Ideal Scenario (Recommended)



Network Diagram – with Static IP addressing (Basic for systems with less RAM)



What you will do (For your understanding)

Install one Linux VM & Windows VM. Make sure you install recent versions of OS as far as possible since I know that you may face problem in downloading these OS and VMs. Convert these to server systems by installing vulnerable versions of FTP Server, ssh server, and http server (but not limited to these).

Please install NMAP & Zenmap to initiate default scanning with default options. Also understand various scanning options allowed in nmap & zenmap. Also install Nessus and configure it with Nessus Professional subscription trial version (7 days trail). Nessus Essentials (Home Feed) licence could be obtained and is perpetual, but has less scanning options and will be able to scan a network up to 16 machines at once. For scanning the network, you have to give the destination network address as 192.168.2.0/24. Also please check and try to understand what is authenticated scanning in Nessus. What are the benefits that it provides compared to the normal scanning method.

Now your job is to use Metasploit for exploiting the vulnerability that you have found out on the above step. Please refer *Chapter 4: Using the Metasploit Framework* from book *Penetration Testing A Hands-On Introduction to Hacking.pdf and also the online videos available in various hacking sites or youtube.*

You have to use Bridge Network or NAT, for setting up this network. Before you carryout this activity, your system has to be totally isolated from internet, by disconnecting the laptop from internet.